Reduction of binary quadratic forms

Florian Trummer
Sina Keller

December 2021

1 Introduction

Within the framework of this seminar we want to look at binary quadratic forms. We will explain what they are and classify them in equivalence classes, for which we want to find canonical representatives. We will also see a surprising and fascinating application, namely how we can use them to solve a specific class of Diophantine equations.

2 First Definitions and Concepts

We will first define some basics in order to know what we work with. Namely we will define what a binary quadratic form in two variable is and what properties and parts it has.

Definition 2.1.

- *We define* ***binary quadratic forms*** *in two variables* $f(x,y) = ax^2 + bxy + cy^2$ *with a,b and c integers.*
- *We define the* ***discriminant*** *of such a form as* $\Delta = b^2 - 4ac$
- *We say a form* $f(x,y)$ ***represents an integer m*** *if there exist integers* x_0, y_0 *such that* $ax_0^2 + bx_0y_0 + cy_0^2 = m$. *We will also use (a,b,c) instead of* $ax_0^2 + bx_0y_0 + cy_0^2 = m$.
- *We say a representation is* ***primitiv*** *if* $gcd(x_0, y_0) = 1$

We note that $\Delta \equiv 1$ or $\Delta \equiv 0 (mod 4)$ and $b \equiv \Delta (mod 2)$.
We will now look at the simplified example $(a,b,c) = (1,0,1)$ and see what holds for this.

Theorem 2.2. *a) If integers a and b exist such that the form* $a^2 + b^2 = m$ *is divisible by any prime p of the form* $4k-1$, *then* $p|a, p|b$ *and* $p^2|m$;

b) the only solutions to $x^2 + y^2 = 2$ are $(x, y) = (\pm 1, \pm 1)$, in which the choices of sign are independent;

c) if p is any prime of the form 4k+1, then there exists a solution $(x, y) = (a, b)$ to the equation $x^2 + y^2 = p$ and the only solutions of this equation are $(x, y) = (\pm a, \pm b)$ and $(\pm b, \pm a)$, where the choices of sign are independent;

d) let $m = 2^t p_1^{r_1} \dots p_s^{r_s}$ be a product of powers of primes, with the p_i all being of the form 4k+1. Let $\{(a_j, b_j)\}$ be the solutions to $x^2 + y^2 = p_j$ for each j. Then, with $i = \sqrt{-1}$, all possible solutions to the equation $x^2 + y^2 = m$ are obtained by writing
$m = (1 + i)^t (1 - i)^t (a_1 + ib_1)^{r_1} (a_1 - ib_1)^{r_1} \cdots (a_s + ib_s)^{r_s} (a_s - ib_s)^{r_s}$ and then rewriting the right-hand side in any form $(a + ib)(a - ib)$.

Now we complete the representation $m = ax^2 + bxy + cy^2$ to the square to get further results: $4am = (2ax + by)^2 - \Delta y^2$.
We see that we get different results for negative and positive values of Δ. For a negative Δ we get a finite number of representations, for a positive Δ we will see that there is an infinite number.

2.1 Transformation and Specification

We consider now a transformation of a form $f(x, y)$:

$$\begin{aligned} x &= \alpha x' + \beta y' \\ y &= \gamma x' + \delta y' \end{aligned} \tag{1}$$

With α, β, γ and δ integers with $\alpha\delta - \beta\gamma \neq 0$. Then the form $f(x, y)$ is transformed into

$$f'(x', y') = a'x'^2 + b'x'y' + c'y'^2 \tag{2}$$

where

$$a' = a\alpha^2 + b\alpha\gamma + c\gamma^2 \tag{3}$$

$$b' = b(\alpha\delta + \beta\gamma) + 2(a\alpha\beta + c\gamma\delta) \tag{4}$$

$$c' = a\beta^2 + b\beta\delta + c\delta^2 \tag{5}$$

$$\Delta' = b'^2 - 4a'c' = (\alpha\delta - \beta\gamma)^2 \Delta \tag{6}$$

Now we can define when two representations of an integer m are equivalent.

Definition 2.3. *$f'(x', y') = (a', b', c')$ is defined to be **equivalent** to a form $f(x, y) = (a, b, c)$ iff f' can be obtained from f by a transformation of the form (1) for which $\alpha\delta - \beta\gamma = +1$; we write $f \sim f'$. This relation is called a **proper equivalence**.*
*In case $\alpha\delta - \beta\gamma = -1$, f and f' are called **improperly equivalent**.*

We can also look at transformations of binary forms in terms of multiplication of matrices. Then we have the classical modular group Γ of 2×2 matrices with integer coefficients and determinant $+1$. It can be constructed as the free product of the two generators S and T defined as follows:
$S = \left(\begin{smallmatrix} 1 & 1 \\ 0 & 1 \end{smallmatrix}\right)$ and $T = \left(\begin{smallmatrix} 0 & -1 \\ 1 & 0 \end{smallmatrix}\right)$.
We see that $S^n = \left(\begin{smallmatrix} 1 & n \\ 0 & 1 \end{smallmatrix}\right)$ and $T^2 = -I$.
Now we want to classify forms up to proper equivalence. We distinguish into cases:

- Δ is a perfect square, then the right side of the completion of the square $(2ax + by)^2 - \Delta y^2$ splits into $(2ax + by + y\sqrt{\Delta}) \cdot (2ax + by - y\sqrt{\Delta})$. We call this the **degenerate case**. We rule out this elementary case;
- $m = 0$, then Δ is a perfect square, therefore we from now on assume $m \neq 0$;
- $\Delta < 0$, then m, a and c must have the same sign since we have $b^2 - 4ac = \Delta$. We call forms with this discriminant **definite forms**. We only want to look at forms in which a and c are positive, we call them **positive definite forms**;
- $\Delta > 0$, they are called **indefinite forms**, since $b^2 - 4ac = \Delta > 0$ a and c can be positive and/or negative;
- a form (k, kn, c) is called **ambiguous**, and the class of such a form is called an **ambiguous class**.

We look at (a,b,a) and see, that it belongs to the following ambiguous class: $(a, b, a) \sim (a, b+2a, b+2a) \sim (b + 2a, -b - 2a, a) \sim (b + 2a, b + 2a, a)$.

2.2 The Modular Group

We now want to take a closer look at Γ.

Theorem 2.4. *Let Γ be the classical modular group, that is, the group of 2×2 matrices with integer coefficients and determinant +1. Γ is the free product group on the generators $S = \begin{pmatrix} 1 & 1 \\ 0 & 1 \end{pmatrix}$ and $T = \begin{pmatrix} 0 & -1 \\ 1 & 0 \end{pmatrix}$.*
That is, any matrix $M \in \Gamma$ can be written as $S^{i_1}T^{j_1}S^{i_2} \cdots S^{i_k}T^{j_k}$ with the i_l and j_l integers. Γ is

also the free product on the generators T and $P = T^3S$. The relations $T^4 = P^3 = I$ are defining relations for Γ.

Proof. It is clear that T and P are of orders 3 and 4, respectively, and that the inverse of $S^n = \begin{pmatrix} 1 & n \\ 0 & 1 \end{pmatrix}$ is $S^{-n} = \begin{pmatrix} 1 & -n \\ 0 & 1 \end{pmatrix}$
The proof that Γ is free on T and S closely resembles the Euclidean algorithm. A given element of Γ is multiplied on the left by powers of S and T until the identity is obtained. Let $M \in \Gamma$ be any such matrix. Then on of M, TM, T^2M, or T^3M is a matrix
$\begin{pmatrix} \alpha & \beta \\ \gamma & \delta \end{pmatrix}$
for which $\beta > 0$ and $\beta \geq |\delta|$. If δ is not zero, we multiply on the left by S^n to get
$\begin{pmatrix} \alpha + \gamma n & \beta + \delta n \\ \gamma & \delta \end{pmatrix}$
We choose n so that we have $|\delta| > \beta + \delta n \geq 0$. Continuing this way, we eventually obtain a matrix with one of the upper right or lower right entries equal to zero. Applying T if necessary, we obtain
$\begin{pmatrix} \alpha & 0 \\ \gamma & \delta \end{pmatrix}$.
Since determinants are multiplicative, we have $\alpha = \delta = \pm 1$. Multiplying by T^2 if necessary, we obtain the matrix
$\begin{pmatrix} 1 & 0 \\ \gamma & 1 \end{pmatrix}$.
Multiplying now by $T^3S^\gamma T$, we obtain the identity, as desired. That Γ is freely generated by T and P follows from the fact that it is freely generated by T and S.
We must show now that no other independent relations hold in Γ. If we had a relation $T^{a_1}P^{b_1}T^{a_2}P^{b_2}\cdots T^{a_n}P^{b_b} = I$ for integers a_i and b_i, then since T^2 commutes with all elements of Γ we may reduce to $P^{b_1}TP^{b_2}\cdots TP^{b_n}T = T^c$ (1.2) with each b_i either 1 or 2 and $c = 0, 1, 2, or 3$. However, both PT and P^2T are matrices
$\begin{pmatrix} \alpha & \beta \\ \gamma & \delta \end{pmatrix}$
for which we have either $\alpha, -\beta - \gamma, \delta \leq 0$ and $\beta + \gamma > 0$ or $\alpha, -\beta - \gamma, \delta \geq 0$ and $\beta + \gamma < 0$; this property is maintained upon multiplication on the right by any element of Γ, but since none of the matrices T^c have this property, no realtion (1.2) can exist. This concludes the proof. □

2.3 The action of Γ on the complex upper-half plane

Now we look at the group Γ as a group of linear fractional transformations of the complex upper half plane, defined as $\mathbf{H} = \{z = x + y\sqrt{-1} \in \mathbb{C} : y > 0\}$, onto itself, with the matrix $M = \begin{pmatrix} \alpha & \beta \\ \gamma & \delta \end{pmatrix}$ corresponding to the mapping $z \mapsto \frac{\alpha z + \beta}{\gamma z + \delta}$.
We see here that the group operation is clearly preserved by this correspondence.

Definition 2.5. *For any group G of injective transformations of a set X to itself, a* ***fundamental domain*** *F is a subset of X such that any point in X can be mapped by some transformation in G to some point in F, and no two points in the interior of F can be mapped to each other by any transformation in G.*

Now we want to see what this F is: Γ is generated, as group of mappings, as the free product of $S(z) = z + 1$ and $T(z) = -1/z$. A fundamental domain F for Γ is the set $F = \{z \in \mathbf{H} : |z| > 1, -1/2 < \mathcal{R}(z) < 1/2\} \cup \{z \in \mathbf{H} : |z| \geq 1, \mathcal{R}(z) = -1/2\} \cup \{z \in \mathbf{H} : |z| = 1, \mathcal{R}(z) \leq 0\}$.
Figure 1 is a illustration of F. Important to note is that the left and right vertical part of F are identified. The same goes for the circle parts. This is illustrated by the || and | signs in the picture. The reason for that is that we can make a similar proof to Theorem 2.4. Then we see that any point in $\mathbf{H}$ is equivalent to some point in F under the action of Γ, and the only equivalent points in F are $i = T(i)$ and $\frac{-1+\sqrt{-3}}{2} = T(S(\frac{-1+\sqrt{-3}}{2}))$.

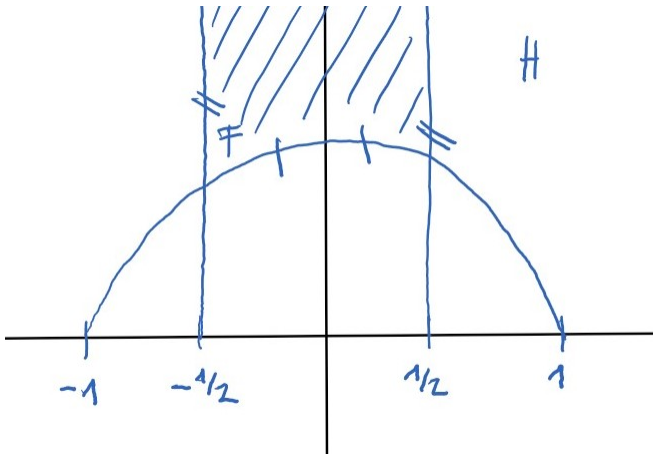

Figure 1: Fundamental domain F

3 Positive Definite Forms

We look at positive definite forms with discriminant $\Delta = -D$. The goal of this section is to determine a canonical representative.

Definition 3.1. *We call a form $f = (a, b, c)$* ***reduced*** *if $|b| \leq a \leq c$.*

Proposition 1. *If $f = (a, b, c)$ is a reduced form of dicriminant -D, then $|b| \leq \sqrt{D/3}$*

Proof. $4b^2 \leq 4ac = b^2 + D$ so $3b^2 \leq D$ □

Theorem 3.2. *The number of reduced forms of a fixed discriminant $-D$ is finite.*

Proof. There are only finitely many candidates for reduced forms since by Proposition 1 the set of possible bs is finite, and each such b determines a finite set of factoring of $b^2 + D$ into $4ac$. □

Theorem 3.3. *Every form f of discriminant -D is equivalent to a reduced form of the same discriminant.*

Proof. We give the reduction algorithm. Let (a, b, c) be a form of discriminant $-D$. If this form is not reduced, an integer δ can be chosen such that $|-b+2c\delta| \leq |c|$. Then $(a, b, c) \sim (c, -b+2c\delta, a-b\delta+c\delta^2) = (a', b', c')$. We now have $|b'| \leq a'$. If $a' \leq c'$, we are done. If not, we repeat the process. Since we only continue the reduction when $c' < a' = c$, and since these are positive integers, the process must terminate, yielding a reduced form. This will become also clear in chapter 3.1. □

Theorem 3.4. *With the exception of*

1) $(a, b, a) \sim (a, -b, a)$

2) $(a, a, c) \sim (a, -a, c)$

no distinct reduced forms are equivalent.

Proof. If (a, b, c) and (a', b', c') are equivalent and reduced, then $a' = a\alpha^2 + b\alpha\gamma + c\gamma^2$ for some α, γ. Then, since $a \geq a'$ (or we would reverse everything), we have

$$a \geq a\alpha^2 + b\alpha\gamma + c\gamma^2 \geq a(\alpha^2 + \gamma^2) + b\alpha\gamma \geq a(\alpha^2 + \gamma^2) - a|\alpha\gamma| \geq a|\alpha\gamma| \tag{7}$$

We conclude that the only allowable cases are $(\alpha, \gamma) = (0, \pm 1), (\pm 1, 0)$, and $(\pm 1, \pm 1$, where the signs in the last are independent.

Case 1. $\alpha = \pm 1, \gamma = 0$. Then $(a, b, c) \sim (a, b + 2a\beta, *)$ or $(a, b - 2a\beta, *)$. The only way, however , to have $|b| \leq a$ and $|b \pm 2a\beta| \leq a$ is to have $\beta = 0$ (in which case the forms are identical) or to have $\beta = \pm 1$ as appropriate and $(a, a, c) \sim (a, -a, c)$

Case 2. $\alpha = 0, \gamma = \pm 1$. Then $(a, b, c) \sim (a, -b \pm 2a\beta, *)$ are equivalent reduced forms. But the center coefficients annot both be small enough unless $\delta = 0, -1, +1$. If $\delta = 0$, then to have (a, b, c) and $(c, -b, a)$ both be reduced, we must have $c = a$ and thus $(a, b, a) \sim (a, -b, a)$. If $\delta = \pm 1$, then $(a, c, c) \sim (c, -c, a)$, but since $a \leq c$, and $c \leq a$, we really have $(a, a, a) \sim (a, -a, a)$

Case 3. $\alpha = \pm 1, \gamma = \pm 1$ independently. In this case we have $a \geq a' \geq a|\alpha\gamma| = a$, so $a = a' = a \pm b + c$. This means $(a', b', c') = (a, b, \pm b)$, but since the form is reduced, we have $a = \pm b$. The reduced equivalent forms are again $(a, a, a) \sim (a, -a, a)$.

□

Theorem 3.5. *Every form of discriminant $-D < 0$ is equivalent to a unique [given the above convention] reduced form.*

Theorem 3.6. *The number of equivalence classes for a given discriminant is finite.*

Definition 3.7. *We define:*

- *the **principal form** as the reduced form $(1, 1, (D-1)/4)$ or $(1, 0, D/4)$ depending on the parity of D.*
- *The **fundamental domain** F for Γ was given as the set*
  $F = \{z \in \boldsymbol{H} : |z| > 1, -1/2 < \mathcal{R}(z) < 1/2\}$
- *the **principal root** of a form f of discriminant $-\Delta$ to be the complex number*
  $\tau = \frac{-b+\sqrt{-D}}{2a}$
  We note that τ is one of the solutions to $ax^2 + bx + c = 0$

Proposition 2. *A form is reduced if and only if its principal root lies in the closure of F.*

Proof. The condition $|b| \leq a$ is equivalent to a condition that $-1/2 \leq \mathcal{R}(\tau) \leq 1/2$. The condition $a \leq c$ is equivalent to

$$1 \leq \frac{c}{a} = \frac{4ac}{4a^2} = \frac{b^2 + D}{4a^2} = \frac{(-b + \sqrt{-D}) \cdot (-b - \sqrt{-D})}{2a \cdot 2a} = \tau\tau' = |\tau| \tag{8}$$

where τ' is the complex conjugate of τ.
Eliminating the $\mathcal{R}(z) = 1/2$ boundary of F is equivalent to choosing a form representative with positive center coefficient, if $|b| = a$, and the forms $(a, 0, a)$ and (a, a, a), the only forms which are nontrivially automorphic to themselves, correspond respectively to principal roots $\tau = \sqrt{-1}$ and $\tau = (-1 + \sqrt{-3})/2$.
These are the special points of the fundamental domain mentioned at the end of Chapter 2.3. A geometric technique for reduction, then, would be:

a) Apply S^n or S^{-n} as necessary to get $|\mathcal{R}(\tau)| \leq 1/2$.

b) Apply T as necessary to get $|\tau| \geq 1$.

c) Repeat as necessary.

□

3.1 Examples

We first list some reduced form representatives of classes and explain how to get to some of those with two different methods.

Δ	h	Reduced Form Representatives of Classes
-3	1	(1,1,1)
-15	2	(1,1,4),(2,1,2)
-23	3	(1,1,6),(2,$\pm$1, 3)
-43	1	(1,1,11)

First we try the 'brute force' method since we know there are only finitely many possible answers. We look at the example $\Delta = -23$ and try to get to the above result only with the condition 1 and 2: $|b| \leq_1 a \leq_2 c$.
From proposition 1 we know that $|b| \leq \sqrt{23}$ therefore $|b| \in [0, 7]$. We now try all the possibilities:

- $b = 0$. Then $23 = 4ac$, since 23 is prime, there are no possible results here.
- $b = 1$. Then $24 = 4ac$ and we get the following possibilities: $(1, \pm 1, 6), (2, \pm 1, 3), (6, \pm 1, 1), (3, \pm 1, 2)$. We can rule out $(6, \pm 1, 1)$ and $(3, \pm 1, 2)$ since they don't follow condition 1 or 2. From theorem 3.4 we know that $(1, +1, 6) \sim (1, -1, 6)$ and we only need to state one of the two equivalent forms.
- $b = 2$. Then $27 = 4ac$, since $4 \nmid 27$, there are no possible results here.
- $b = 3$. Then $32 = 4ac$ and we get the forms $(1, \pm 3, 8), (8, \pm 3, 1), (2, \pm 3, 4), (4, \pm 3, 2)$. All of them don't follow condition 1 or 2 so they are not reduced.
- $b = 4$. Then $39 = 4ac$, since $4 \nmid 39$, there are no possible results here.
- $b = 5$. Then $48 = 4ac$ and we get the forms $(1, \pm 5, 12), (12, \pm 5, 1), (2, \pm 5, 6), (6, \pm 5, 2), (3, \pm 5, 4), (4, \pm 5, 3)$. All of them don't follow condition 1 or 2 so they are not reduced.
- $b = 6$. Then $59 = 4ac$, since $4 \nmid 59$, there are no possible results here.
- $b = 7$. Then $72 = 4ac$ and we get the forms $(1, \pm 7, 18), (18, \pm 7, 1), (2, \pm 7, 9), (9, \pm 7, 2), (3, \pm 7, 6), (6, \pm 7, 3)$. All of them don't follow condition 1 or 2 so they are not reduced.

We end up with $(1, 1, 6)$ and $(2, \pm 1, 3)$ as expected.

We now try the method of reducing a form by the algorithm mentioned in the proof of Theorem 3.2.
We look at the example $\Delta = -3$. We take the form $(a, b, c) = (7, 5, 1)$ and see that this is not a reduced form. We use the algorithm given in 3.2 and find a δ such that $|-b+2c\delta| \leq |c|$. With $\delta = 2$

we have $|-5+2\cdot 2| \leq |1|$ and therefore we find $(7,5,1) = (a,b,c) \sim (c, -b+2c\delta, a-b\delta+c\delta^2) = (1, -5+4, 7-10+4) = (1,-1,1) = (a',b',c')$. From Theorem 3.4 we know that $(1,-1,1) \sim (1,1,1)$ so we get exactly what we expected. Since $1 \leq 1$ we are done now.

4 Indefinite Forms

Now we'll examine indefinite binary quadratic forms, thus forms of the type

$$f(x, y) = ax^2 + bxy + cy^2 \tag{9}$$

such that the discriminant is positive, i.e.

$$D := \Delta := b^2 - 4ac > 0 \tag{10}$$

As in the case of positive definite forms, we want to find canonical forms for the equivalence classes under the equivalence relation defined previously.
We will find that reduced forms are not unique for a given equivalence class, opposed to the case of positive definite forms, but that for each equivalence class the reduced forms form cycles.

4.1 Reduction & cycles

From now on all considered binary quadratic forms are indefinite unless stated otherwise.

Definition 4.1. *We call a form* ***reduced*** *if it fulfills the following 2 conditions:*

1.
$$0 < b < \sqrt{D} \tag{11}$$

2.
$$\sqrt{D} - b < 2|a| < \sqrt{D} + b \tag{12}$$

Lemma 4.2. *Any indefinite form is equivalent to a reduced form of the same discriminant.*

Proof. Using the following algorithm on a given form f defined by (a, b, c) yields a reduced form f' such that $f \sim f'$:

1. If (a, b, c) is reduced then stop the algorithm.
2. Choose $\delta \in \mathbb{Z}$ such that
$$\sqrt{D} - 2|c| < -b + 2c\delta < \sqrt{D} \tag{13}$$
Define f' to be the form represented by $(c, -b + 2c\delta, a - b\delta + c\delta^2)$.
3. If $|a - b\delta + c\delta^2| < |c|$ we repeat step 2 with f'.

□

Claim This algorithm stops after finitely many repetitions of step 2. The resulting form f' is reduced and $f \sim f'$.

Proof. In each repetition of step 2 the term $|a - b\delta + c\delta^2|$ gets strictly smaller than the one before. Since the first one is bounded by $|c|$, this can happen only finitely many times, thus the algorithm stops after finitely many steps. We get a form (A, B, C) such that $|A| \leq |C|$ (otherwise the algorithm would not stop) and $\sqrt{D} - 2|A| < B < \sqrt{D}$ by the choice of δ and the definition of f'.
Thus $\sqrt{D} - B < 2|A|$. Together with $|\sqrt{D} - B||\sqrt{D} + B| = |D - B^2| = 4|A||C|$ this leads to $|\sqrt{D} + B| > 2|C|$.
Putting everything together we get $|\sqrt{D} + B| > 2|C| > 2|A| > \sqrt{D} - B$. This shows (12). Now we see that if B was nonpositive, we would have $\sqrt{D} - B \geq |\sqrt{D} + B|$, which contradicts the inequality above. Thus B is positive, so we get $0 < B < \sqrt{D}$ and therefore (A,B,C) is reduced.

In each repetition of step 2. we have

$$(a, b, c) \sim (c, -b + 2c\delta, a - b\delta + c\delta^2) \tag{14}$$

using the matrix $\begin{pmatrix} 0 & -1 \\ 1 & \delta \end{pmatrix}$ for the reduction transformation. Since $\sim$ is transitive, we have $(a, b, c) \sim (A, B, C)$.

The discriminant of f' which we get in an iteration of step 2 is
$D' = b'^2 - 4a'c' = (-b + 2c\delta)^2 - 4c(a - b\delta + c\delta^2) = -b^2 + 4c^2\delta^2 - 4bc\delta - 4ca + 4cb\delta - 4c^2\delta^2 = b^2 - 4ac = D$.
Thus our algorithm yields forms of the same discriminant, thus also the reduced form at the end of the algorithm has the same discriminant as f. □

□

Now we'll give an example of a reduction using this algorithm.

Example Look at the form $f(x, y) = 6x^2 + 42xy + 11y^2$. We have $D = 1500$, so f is not reduced and we go to step 2.
We're looking for an integer δ such that $16.73 \simeq \sqrt{D} - 2|c| < -b + 2c\delta = 22\delta - 42 < \sqrt{D} \simeq 38.73$ and we find $\delta = 3$. So we get the form $(c, -b + 2c\delta, a - b\delta + c\delta^2) = (11, 24, -21) =: (A, B, C) \sim (a, b, c)$.
For this form we have $0 < 24 = B = 38.73 \simeq \sqrt{D}$ and also $\sqrt{D} - B \simeq 14.72 < 22 = 2|A| < 62.73 \simeq \sqrt{D} + B$. So (A, B, C) is reduced and f equivalent to a reduced form.

Definition 4.3. *Two reduced forms (a, b, c) and (c, b', c') are called **adjacent** if $b + b' \equiv 0 \pmod{2c}$.*

Lemma 4.4. *Let $f = (a, b, c)$ be a reduced form. Then there exist exactly one adjacent form with the same discriminant on the right and on the left. They are equivalent to (a, b, c).*

Proof. We will prove the statement for the adjacent form on the left. The proof for the adjacent form on the right follows analogously.

Let therefore $f' = (A, B, a)$ be adjacent to (a, b, c). We distinguish the cases depending on a. Since f is reduced we have $b < \sqrt{D} = \sqrt{b^2 - 4ac}$ and thus $a \neq 0$. Now assume $a > 0$.

By definition of an adjacent form exists an integer k such that

$$B = 2ak - b$$

Since f' is reduced and has discriminant D we have

$$\sqrt{D} - B < 2|a| < \sqrt{D} + B$$

The first inequality leads to

$$\sqrt{D} + b - 2ak < 2|a| \tag{15}$$

Solving for k yields

$$k > \frac{\sqrt{D} + b}{2a} - 1$$

The other condition which f' fulfills since it is reduced ($0 < B < \sqrt{D}$) gives us an upper bound for k:

$$2ak - b < \sqrt{D} \iff k < \frac{\sqrt{D} + b}{2a}$$

Putting together our bounds for k we find

$$\frac{\sqrt{D} + b}{2a} - 1 < k < \frac{\sqrt{D + b}}{2a} \tag{16}$$

Thus k is fixed uniquely. Therefore also $B = 2ak - b$ is fixed uniquely.

Moreover we have that f' and f have the same discriminant D:

$$b^2 - 4ac = D = B^2 - 4Aa$$

Solving for A yields

$$A = \frac{B^2 - D}{4a} \tag{17}$$

Since B is determined uniquely, so is A and thus f'.

Now let $a < 0$. Setting $a' = -a$ we find a unique k' satisfying (16). Setting $k' = -k$ we see that $ak = a'k'$, thus k is uniquely determined and by the same reasoning as before we find that B, A and therefore f' are uniquely determined. Lastly we show that these forms are equivalent. Let therefore k be defined as before and $A = \begin{pmatrix} k & 1 \\ -1 & 0 \end{pmatrix}$. Let this transformation work on f using the equations (3), (4) and (5). We get $f* = (a', b', c') = (k^2a - bk + c, 2ak - b, a)$. Since $det(A) = 1$ we have that f and the resulting form $f*$ are equivalent. In particular they have the same discriminant. Moreover $c' = a$ and $b' + b = 2ak$ we have that $f* \sim f$ and by uniqueness we thus have that $f*$ is the adjacent form on the left to f. □ □

Lemma 4.5. *The number of reduced forms (a, b, c) of a given discriminant is finite.*

Proof. Condition 1 in the definition of a reduced form yields that b can only take finitely many values. For each such b we have only finitely many options to factorise $\frac{D-b^2}{4} = ac$ in a and c. Therefore we have in total only finitely many possible reduced forms. □

These 2 lemmas lead to the following proposition:

Proposition 4.6. *The set of reduced forms of a given discriminant can be partitioned into cycles of adjacent forms. Moreover, the forms in a cycle are all equivalent to each other.*

Proof. Let (a, b, c) be a reduced form. Lemma 4.4 yields us that we can find exactly one reduced form on the right of f. Repeating this argument for the newly found reduced form leads us to a sequence of reduced adjacent forms. But the set of possible reduced forms for the given discriminant is finite. So the sequence has to return to (a, b, c), and by uniqueness of the successor we have found a cycle with one generator.
Since lemma 4.4 gives us that adjacent forms are equivalent, and the equivalent relation is transitive, we have that all reduced adjacent forms in a cycle are equivalent.
If we have remaining reduced forms, we restart this process and find other cycles which are generated by these reduced forms. Since there are only finitely many reduced forms, this process is finite and we get the desired partition in cycles of adjacent reduced forms.

□

This proves one direction of the important theorem

Theorem 4.7. *Two reduced forms are equivalent if and only if they are in the same cycle.*

A proof for the other direction can be found in the Appendix.

Example Examination shows that we find 4 reduced forms with discriminant $D = 24$: $(1, 4, -2), (-2, 4, 1), (-1, 4, 2)$ and $(2, 4, -1)$. We see that the first 2 and the second 2 forms are adjacent and each pair forms a cycle. So we have the two cycles $(1, 4, -2), (-2, 4, 1)$ and $(2, 4, -1), (-1, 4, 2)$

4.2 Pell's equation

We have seen that, for a given discriminant, the reduced forms build cycles. Forms are equivalent to each other if and only if they lie in the same cycle. In this chapter we will see a fascinating application of this: Using our theory on reduced binary quadratic forms we can find solutions to some diophantine equations, called Pell's equation. We will examine the following example

$$x^2 + 8y^2 = 4 \tag{18}$$

Definition 4.8. *For a fixed integer D and x, y integers, we call the equation $x^2 - Dy^2 = 4$* ***Pell's equation****.*

The following lemma will be useful:

Lemma 4.9. *Every reduced form f in a nontrivial cycle admits an automorphism.*

Proof. There exists a transformation matrix A_1 which transforms f to its adjacent f'. We can move through the whole cycle of adjacent matrices until we return to f, and obtain the transformation matrices A_i for $i = 1, .., m$. Thus the matrix product of $\Pi_{i=1}^{m} A_i$ takes f to f and is thus an automorphism. □

Definition 4.10. *We define the* ***principal root*** *ω of an indefinite form (a, b, c) to be $\omega = \frac{-b+\sqrt{\Delta}}{2a}$.*

Theorem 4.11. *Let (a, b, c) be a primitive binary quadratic form with discriminant D. Then Pell's equation $x^2 - Dy^2 = 4$ has a solution. Moreover, the solutions to Pell's equation give automorphisms of (a, b, c), and vice-versa.*

Proof. For the principal root ω we have $a\omega^2 + b\omega + c = 0$.
By Lemma 4.9 there exists an automorphism $\omega = \frac{\omega\alpha+\beta}{\gamma\omega+\delta}$. Algebraic transformations yield $\gamma\omega^2 + (\delta - \alpha)\omega - \beta = 0$. Since f is primitive this leads to $\gamma\omega^2 + (\delta - \alpha)\omega - \beta = k(a\omega^2 + b\omega + c)$ for an integer k. So we find

$$Dk^2 = k^2 b - 4ack^2 = (\delta - \alpha) + 4\gamma\beta \tag{19}$$

Since adjacent matrices are equivalent to each other, the transformation matrices have determinant 1, so $\alpha\delta - \gamma\beta = 1$. Plugging this in equation (19) we get:

$$(\alpha + \delta)^2 - Dk^2 = 4 \tag{20}$$

Setting $x = \alpha + \delta$ and $y = k$ we get a solution to Pell's equation.

On the other hand, a solution x, y to Pell's equation leads to an automorphism of the form (a, b, c). Define, for this purpose,:

$$\alpha = \frac{x - by}{2}$$

$$\beta = -cy$$

$$\gamma = ay$$

$$\delta = \frac{x + by}{2}$$

and the transformation τ acting on a, b and c as given in equations (3), (4) and (5) respectively. We'll check $\tau(a) = a$, the equalities for $\tau(b) = b$ and $\tau(c) = c$ follow analogously.
Using equation (3) yields:

$$\tau(a) = a\alpha^2 + b\alpha\gamma + c\gamma^2 = \frac{a}{4}x^2 + \frac{a}{4}(-b^2 + 4ac)y^2$$

where we plugged in the definitions of α, β and γ and regrouped the terms. Using the fact that x, y solve Pell's equation leads to:

$$a' = \frac{a}{4}x^2 + \frac{a}{4}(-Dy^2) = \frac{a}{4}x^2 + \frac{a}{4}(4 - x^2) = a.$$

□ □

Example So let's tackle our initial question 18 of a solution to the equation $x^2 - 8y^2 = 4$. First we have to find a form f' with determinant $D = 8$. This form leads, using our standard algorithm, to a reduced form f with determinant D.Thus we find the reduced form $f = (1, 2, -1)$. Now we can cycle backward in order to find an automorphism to f by proceeding as in Lemma 4.11.

Firstly we're looking for an integer k_1 fulfilling the inequality given by (16):

$$\frac{\sqrt{D} + b}{2a} - 1 = \frac{\sqrt{8} + 2}{2} - 1 < k_1 < \frac{\sqrt{8} + 2}{2} = \frac{\sqrt{D} + b}{2a}$$

We thus find $k_1 = 2$, $b_1 = 2ak_1 - b = 2$ and $a_1 = \frac{b_1^2 - D}{4a} = -1$, so $f_1 = (-1, 2, 1)$.

For f_1 we have $a_1 < 0$, thus we set $a_1' = -a_1$:

$$\frac{\sqrt{D} + b_1}{2a_1'} - 1 = \frac{\sqrt{8} + 2}{2} - 1 < k_2' < \frac{\sqrt{8} + 2}{2} = \frac{\sqrt{D} + b}{2a'}$$

Therefore $k_2 = -k_2' = -2$, $b_2 = b_1 - 2ak_2 = 2$ and $a_2 = \frac{b_2^2 - D}{4a_1} = 1$. Therefore $f_2 = (1, 2, -1) = f$ and we have found the whole cycle.

As seen in the proof of Lemma 4.4 the transformation matrix yielding f_i is

$$A_i := \begin{pmatrix} k_i & 1 \\ -1 & 0 \end{pmatrix}$$

Thus the product of all transformation matrices is an automorphism A on f:

$$\begin{pmatrix} \alpha & \beta \\ \gamma & \delta \end{pmatrix} = A = A_1 A_2 = \begin{pmatrix} 2 & 1 \\ -1 & 0 \end{pmatrix} \begin{pmatrix} -2 & 1 \\ -1 & 0 \end{pmatrix} = \begin{pmatrix} -5 & 2 \\ 2 & -1 \end{pmatrix}$$

Having found an automorphism on f we can now, according to Lemma 4.11, find a solution to Pell's equation. As in the proof of Lemma 4.11 we set $x = \alpha + \delta = -6$ and look for y such that $\gamma\omega^2 + (\delta - \alpha)\omega - \beta = y(a\omega^2 + b\omega + c) = y(\omega^2 + 2\omega - 1)$ where ω is as usual the principal root of f. Plugging in the values of our automorphism we get $2\omega^2 + 4\omega - 2 = y(\omega^2 + 2\omega - 1)$. Therefore we have found $y = 2$.

We can check that the solution $(x, y) = (-6, 2)$ we found is correct: $x^2 - 8y^2 = 36 - 8 \cdot 4 = 4$.

5 Appendix

5.1 Continued fractions

We recall the main theorem we want to prove:

> Two reduced forms are equivalent if and only if they are in the same cycle.

In order to do this, we will need the concept of continued fractions and some lemmas, which will be stated without proof. However, the interested reader can find them in [1].

Lemma 5.1. *A given discriminant and principal root characterise a reduced form uniquely.*

Definition We define a *simple continued fraction* expansion of $x \in \mathbb{R}$ to be a function

$$x = f(a_0, ..., a_N) = a_0 + \cfrac{1}{a_1 + \cfrac{...}{+\cfrac{1}{a_N}}} =: [a_0, .., a_N]$$

where $\forall i = 0, .., N : a_i \in \mathbb{Z}$ and $\forall i = 1, .., N : a_i > 0$.

Definition We call a simple continued fraction *periodic* if

$$\exists I, J \in \mathbb{N} : \forall i \geq I : a_i = a_{i+J}$$

In this case we write this as $[a_0, ..., a_{I-1}, *a_I, ..., *a_{I+J-1}]$

Lemma 5.2. *If ω is an irrational root of a quadratic equation with integer coefficients, then the simple continued fraction for ω is periodic.*

Lemma 5.3. *A purely periodic continued fraction is unique for a given quadratic irrational.*

Lemma 5.4. *A transformation $y = \frac{\alpha x+\beta}{\gamma x+\delta} \in \Gamma$, where Γ is the modular group, can be written in the language of continued fractions as*

$$y = [\pm t, a_1, ..., a_{2r}, \pm u, x]$$

where $\forall i = 1, .., 2r : a_i > 0$.

Proof of theorem 4.7 Since we've already shown that forms in the same cycle are equivalent, we will focus on the reverse direction. Let thus $f = (a, b, c)$ and $f' = (a', b', c')$ be equivalent reduced forms with $a, a' > 0$ and such that their principal roots ω, ω' are positive proper fractions (i.e. they lie in $[0, 1)$)

.

If we look at the transformation $A = \begin{pmatrix} \alpha & \beta \\ \gamma & \delta \end{pmatrix}$ which transfers f to f' (A exists since the forms are equivalent), we have $\omega' = \frac{\alpha\omega+\beta}{\gamma\omega+\delta}$. By Lemma 5.4 there exist $t, a_1, ..., a_{2r}, u$ such that

$$\omega' = [\pm t, a_1, ..., a_{2r}, \pm u, \omega] \tag{21}$$

Since ω' is a positive proper fraction, we have $t = 0$. The same holds for the continued fraction of ω, so using Lemma 5.2 we have $\omega = [*d_1, ..., *d_{2m}]$. Plugging this in (21) yields

$$\omega' = [\pm t, a_1, ..., a_{2r}, \pm u + d_1, *d_2, .., *d_{2m}, *d_1]$$

Lemma 5.3 yields that the periodic part of the expansion of ω' is a cyclic permutation of the one of ω. Since cycling forward means cycling the periodic part, we have that, by cycling forward from f, we find a reduced form f^* with principal root ω'. Since f^* and f' have same discriminant and principal root, we have $f^* = f'$ by Lemma 5.1, which concludes the proof. □

References

[1] Binary Quadratic Forms, Classical Theory and Modern Computations by D.A. Buell (Springer-Verlag 1989)